Department of Veterans Affairs
Washington, DC 20420

VA Directive 0734
Transmittal Sheet
July 7, 2017

Classified National Security Information Program

1. REASON FOR ISSUE: This Directive establishes Department-wide authorities and responsibilities for the Department of Veterans Affairs (VA) Classified National Security Information (CNSI) Programs.

2. SUMMARY OF CONTENT: This policy establishes roles and responsibilities for VA's CNSI Programs. It includes policies involving access to CNSI that resides on Automated Information Systems (AIS). The policy shall ensure that the number of persons granted access to classified information meets the mission needs of the agency while also satisfying operational and security requirements. VA shall protect CNSI and ensure implementation of a uniform system for managing CNSI.

3. RESPONSIBLE OFFICE: Operations, Security, and Preparedness (OSP), 007, Office of Emergency Management and Resilience (OEMR) (07A).

4. RELATED HANDBOOK: None

5. RESCISSION: None

CERTIFIED BY:

/s/
Dat P. Tran
Acting Assistant Secretary for
Office of Enterprise Integration

BY DIRECTION OF THE
SECRETARY OF VETERANS AFFAIRS

/s/
Kevin T. Hanretta
Acting Assistant Secretary for
Operations, Security, and Preparedness

This page left intentionally blank.

Classified National Security Information Program

1. PURPOSE

Executive Order (E.O.) 13526 "Classified National Security Information" signed by President Barack Obama on December 29, 2009, prescribed a uniform system for classifying, safeguarding, and declassifying classified information. The Director of the Information Security Oversight Office (ISOO), under direction of the Archivist, National Archives and Records Administration (NARA) and in consultation with the National Security Advisor, issued guidance to agencies in, Parts 2001 and 2003 Title 32, Code of Federal Regulations (C.F.R.). VA Directive 0734 implements E.O. 13526 and adheres to final rule guidance codified in 32 C.F.R., Parts 2001 and 2003.

2. POLICY

This policy establishes roles and responsibilities for the Department of Veterans Affairs' (VA) Classified National Security Information (CNSI) Programs. It includes policies involving access to CNSI that resides on Automated Information Systems (AIS). In accordance with E.O. 13526, this policy outlines the procedures to ensure that the number of persons granted access to classified information meets the mission needs of the VA while also satisfying operational and security requirements and needs. VA shall protect CNSI and ensure implementation of a uniform system for managing CNSI.

3. RESPONSIBILITIES

a. **The Secretary of Veterans Affairs.** Has overall responsibility for VA's management and implementation of the CNSI program established under E.O. 13526. The Secretary delegates this responsibility to the Assistant Secretary for Operations, Security, and Preparedness (AS/OSP).

b. **Assistant Secretary, Operations Security and Preparedness (AS/OSP).** Serves as the Department's Senior Agency Official (SAO) responsible for the implementation of E.O.13526 and for directing and administering VA's CNSI Program. As VA's SAO, the AS for OSP shall:

(1) Establish and maintain procedures that will enable the prompt identification of any existing practice or condition that fails to afford adequate safeguarding of all classified information in the possession of VA, and taking prompt and effective action to correct any deficiency noted or reported.

(2) Establish and maintain security education and training programs.

(3) Establish and maintain an ongoing VA-wide self-inspection program. The self-inspection program provides the SAO with an assessment of VA's CNSI Program. The SAO is required to report this information annually to the ISOO.

(4) Establish procedures to prevent: a) unauthorized access to classified information and/or b) damage to national security.

(5) Ensure cleared employees who have access to classified information have a need-to-know.

(6) Account for the costs associated with classification related activities. This information shall be reported to the Director of ISOO annually. ISOO reports this information annually to the President of the United States.

(7) Ensure that safeguarding practices are continually reviewed, eliminating those that are duplicative and unnecessary. This will ensure VA is always using best security practices.

(8) Administratively withdraw or downgrade security clearances without prejudice for any individual who no longer requires access to CNSI. This includes withdrawal or downgrading of security clearances when CNSI access in no longer needed in connection with the performance of the individual's official duties and obligations.

(9) Maintain a foreign travel program that requires all VA employees with a security clearance (Secret/Top Secret) to provide notice of all foreign travel, conducted for either official or personal purposes. Foreign travel is defined as travel outside the United States and its Territories. Such employees may be required to receive a travel briefing prior to foreign travel and shall be subject to a security debrief upon completion of foreign travel in accordance with VA Directive 0736.

(10) Promptly and fully investigate the circumstances of any violation/ infraction, or possible compromise of classified information including notifying the originating agency and coordinating any follow-up investigation or request for information related to the incident.

(11) Take all appropriate actions pertaining to the loss or possible compromise of CNSI, including notifying the originating agency, the ISOO, VA Office of Inspector General (OIG) and/or federal law enforcement agencies as necessary.

(12) Ensure all classification markings in the electronic environment are subject to all requirements in accordance with 32 C.F.R. Part 2001.23.

(13) Safeguard all classified networks in VA and ensures that all safeguarding procedures are being enforced.

(14) Oversee VA's Sensitive Compartmented Information (SCI) program in accordance with Intelligence Directives, Director of Central Intelligence Directives (DCID), Intelligence Community Directives (ICD), and Intelligence Community Policy Guidance (ICPG).

(15) Ensure every security clearance holder in VA is notified of the changes in Presidential Policy Directive-19 (PPD-19),"Protecting Whistleblowers with Access to Classified Information."

(16) Issue courier letters to cleared employees for the purpose of receiving and transporting CNSI.

(17) Ensure that performance plans used to rate an employee's performance includes provisions regarding the management of classified information as a critical element for employees with a security clearance.

c. **Deputy Assistant Secretary, Office of Emergency Management and Resilience (DAS/OEMR)**. The AS for OSP further delegates authority to the DAS OEMR to serve as the Department's SAO.

d. **Under Secretaries, Assistant Secretaries, and Other Key Officials.** VA Under Secretaries, Assistant Secretaries and Other Key Officials shall support OSP with implementing all rules, regulations, and policies regarding CNSI.

e. **Assistant Secretary, Office of Information and Technology (AS/OI&T).** AS/OI&T will provide sustainment funding from Information and Technology Operations and Services.

f. **Office of Inspector General (OIG).** OIG shall determine which OIG positions are national security positions in accordance with The Inspector General Act of 1978. OIG shall investigate reports of fraud, waste, and abuse and assist OSP with investigations involving the misuse or unauthorized disclosure of classified information.

g. **Assistant Secretary, Human Resources and Administration (AS/HRA).** The AS/HRA will ensure all positions are designated with the appropriate risk or sensitivity level in accordance with the Position Designation Automated Tool (PDAT) and ensure that each appointee and employee receives a background investigation commensurate with the position risk or sensitivity level.

h. **Cleared Employee.** All cleared personnel who possess access to CNSI at the Secret (S), Top Secret (TS), and/or TS/Sensitive Compartmented Information (SCI) level shall abide by: E.O. 13526; 32 C.F.R. Parts 2001 and 2003 and implementing directives; E.O. 12968, "Access to Classified Information", dated August 4, 1995; E.O.13467, "Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Information," dated June 30, 2008; E.O. 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," dated October 7, 2011; Intelligence Community Directive 700, "Protection of National Intelligence," dated June 7, 2012; VA Insider Threat Directive

0327; 5 C.F.R. Part 732 - National Security positons, dated January 1, 2012; and all other federal regulations, and policies related to CNSI.

4. REFERENCES. Nothing in this Policy shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended, or the National Security Act of 1947, as amended. ‘‘Restricted Data’’ and ‘‘Formerly Restricted Data’’ shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued under that Act.

a. E.O. 10450, “Security Requirements for Government Employment,” dated April 27, 1953.

b. E.O. 12968, “Access to Classified Information,” dated August 4, 1995.

c. Office of Management and Budget Memorandum “Reciprocal Recognition of Existing Personnel Security Clearances,” dated December 12, 2005.

d. E.O. 13467, “Reforming Process Related to Suitability for Government Employment, Fitness for Contactor Employees, and Eligibility for Access to Classified National Security Information,” dated June 30, 2008.

e. E.O. 13526, “Classified National Security Information,” dated December 29, 2009.

f. E.O. 13587, “Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information,” dated October 7, 2011.

g. 5 C.F.R., Part 731 “Suitability,” dated April 15, 2008.

h. 5 C.F.R., Part 732 “National Security Positions”, dated January 01, 2012.

i. Title 32 C.F.R., Parts 2001 and 2003 “Classified National Security Information,” dated June 28, 2008.

j. “National Security Act of 1947, As Amended”, dated July 26, 1947.

k. PPD-19,”Protecting Whistle Blowers with Access to Classified Information,” dated October 10, 2012.

l. White House Memorandum, “Foreign Travel by U.S. Officials,” dated March 27, 1989.

m. ICD 700, “Protection of National Intelligence,” dated June 7, 2012.

n. ICD 701, “Security Policy Directive for Unauthorized Disclosures of Classified Information,” dated March 14, 2007.

o. ICD 704, “Personnel Security Standards and Procedures Governing Eligibility Access to Sensitive Compartmented Information, and other Control Access Program Information,” dated October 1, 2008.

p. ICD 705, “Sensitive Compartmented Information Facilities,” dated May 26, 2010.

q. ICD 710, “Classification Management and Control Markings System,” dated June 21, 2013.

r. Intelligence Community Policy Memorandum Number 2007-700-3, Director of National Intelligence Foreign Travel Reporting Form.

s. VA Directive 0710, “Personnel Security and Suitability Program” dated June 4, 2010.

5. DEFINITIONS

a. **Access.** The ability or opportunity to gain knowledge of classified information.

b. **Agency.** Any “Executive Agency” as define in U.S.C. 105 ”Military Department” as defined in 5 U.S.C 102”; and any other entity within the executive branch that comes into possession of classified information.

c. **Automated Information Systems.** An assembly of computer hardware, software, or firmware configured to collect, create, communicate, commute, disseminate, process, store, or control data or information.

d. **Authorized Person.** A person who has a favorable determination of eligibility for access to classified information, has signed an approved nondisclosure agreement, and has a need to know for the specific classified information in performance of official duties.

e. **Classification.** The act or process by which information is categorized based on content and determined to be classified information.

f. **Classified National Security Information (or Classified Information).** Information that has been determined pursuant to E.O. 13526” Classified National Security Information” or any predecessor order to require protection against unauthorized disclosure and is marked to indicate the classified status when in documentary form.

g. **Cleared Employee.** A person who has been granted access to classified information, other than the President and Vice President, employed by, detailed, or assigned to a department or agency, including members of the armed forces; an expert

or consultant for a department or agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of a department or agency including all subcontractors, personal services contractors; or any other category of persons who act on behalf of a department or agency as determined by the appropriate department or agency head.

h. **Courier.** An individual authorized to transport classified information.

i. **Damage to the National Security.** Harm to national defense or foreign relations of the U.S. from the unauthorized disclosure of information. Such aspects of the information taking into considerations, such as the sensitivity, value, utility, and provenance of that information.

j. **Document.** Any recorded information, regardless of the nature of the medium or the method or circumstances of recording.

k. **Information.** Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics that is owned by is produced by or for, or is under the control of the U.S. Government. "Control" means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

l. **Infraction.** Any knowing, willful, or negligent action contrary to the requirements of E.O. 13526:"Classified National Security Information", or this implementing Directive that does not constitute a "violation" as defined below.

m. **National Security.** The national defense or foreign relations of the U.S.

n. **Need-to-know.** A determination within the executive branch in accordance with directives issued pursuant to this order that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

o. **Network.** A system of two or more computers that can exchange data or information.

p. **Position Designation System and Automated Tool.** The Office of Personnel Management (OPM) position designation process used to determine the appropriate level of investigations for National Security and Public Trust position.

q. **Presidential Policy Directive (PPD) 19.** PPD-19, signed by President Barack Obama, is designed to ensure that employees who service in the Intelligence Community or have access to classified information can effectively report waste, fraud, and abuse, while protecting classified information.

r. **Principal Officer.** The official in charge of an organization designated as a Principal Officer.

s. **Safeguarding.** Measures and controls that are prescribed to protect classified information from loss compromise or alteration.

t. **Security Clearance.** A determination that a person is eligible for access to classified information.

u. **Sensitive Compartmented Information (SCI).** National Security Information classified as Confidential, Secret, or Top Secret and because it is derived from intelligence sources, methods, or analytical processes; it requires special handling and additional protection measures which are contained within formal access control systems (compartments) established by the Office of the Director of National Security.

v. **Sensitive Compartmented Information Facility (SCIF).** An area, room, group of rooms, buildings, or installation certified and accredited as meeting Director of National Intelligence security standards for the processing, storage, and/or discussion of SCI.

w. **Self- Inspection.** The internal review and evaluation of individual VA activities and VA as a whole, with respect to the implementation of the program established under Executive Order 13526 “Classified National Security Information, and 32 C.F.R., Part 2001”Classified National Security Information”.

x. **Senior Agency Official (SAO).** The official designated by the Secretary under section 5.4 (d) of E.O. 13526 “Classified National Security Information,, to direct administer VA's program under which information is classified, safeguarded, and declassified.

y. **Violation.** Any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information. Any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of E.O. 13526”Classified National Security Information”, or the implementing directives. Any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of E.O.